June 15, 2004

Federal Trade Commission
Office of the Secretary, Room H-159 (Annex J)
600 Pennsylvania Avenue, NW
Washington, DC 20580

RE: FACTA Identity Theft Rule, Matter No. R411011

To Whom It May Concern:

As a leader in the financial services industry ("the industry"), Fifth Third Bancorp[1] ("Fifth Third") welcomes the opportunity to comment on the proposal issued by the Federal Trade Commission (FTC) regarding the definitions of "identity theft" and "identity theft alerts" as well as related provisions.

Fifth Third appreciates and supports the overall objectives of the proposal to assist consumers and the financial industry in combating the rapidly growing problem of "identity theft". However, we are concerned that certain provisions, as proposed, may place an undue burden on financial institutions.

Definition of "Identity Theft" and "Identifying Information"

The "Fair and Accurate Credit Transactions Act" (FACTA) defines "identity theft" to mean "a fraud committed using the identifying information of another person, subject to such further definition as the [FTC] may prescribe." As proposed, "identity theft" is defined as "a fraud committed or attempted using the identifying information of another person without lawful authority."

We believe the definition of "identity theft" should only include actual instances of "identity theft" versus attempted or threatened actions in order that limited resources may be dedicated to assisting true victims. Definitions should be clear that other types of fraudulent account use, such as misuse of a credit card by an unauthorized party, are not considered identity theft and thus are not subject to compliance with regulations pertaining to the "red flag" programs, identity theft reports, and the requirements of Section 609(e) of the FCRA.

The FTC also indicates that an expanded definition of "identity theft" would be helpful for consumers "who have learned of attempts by an identity thief and want to…place an initial fraud alert" in their consumer files.

[1] Fifth Third Bancorp provides banking, investment and electronic payment processing services to 5.7 million customers through 17 affiliates in Ohio, Kentucky, Indiana, Michigan, Illinois, West Virginia, Tennessee and Florida. With $91 billion in assets, Fifth Third is among the top 15 largest bank holding companies in the nation and among the ten largest in market capitalization.

While we believe it would be appropriate for an initial alert to be placed in a consumer's credit file if he or she is the subject of an attempted identity theft, it is not necessary to expand the definition of "identity theft" in order to achieve this goal. Specifically, the FCRA permits a consumer who "asserts in good faith a suspicion that the consumer has been or is about to become a victim of fraud or related crime" to place an initial alert in his or her file; there is no requirement that the consumer be a victim of identity theft. Therefore, an expanded definition of "identity theft" is not necessary to achieve the FTC's objective in this respect

In regard to "identifying information", the proposed rule would require that "identity theft" involve the use of the "identifying information" of another person. The FTC defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual." We believe that the definition of "identity theft" should reflect only situations in which a criminal assumes a victim's identity to control existing accounts or establish new accounts.

Therefore, we strongly urge the FTC to reconsider what types of information would qualify as "identifying information." We believe "identifying information" should be of the types of information that allow a criminal to masquerade as a victim with respect to new accounts or alternation of existing accounts. Unauthorized use of an existing account should not rise to the level of becoming an "identity theft."

Identity Theft Reports

The FCRA provides identity theft victims the ability to block the false information resulting from the identity theft from their credit histories. We agree with this approach as a meaningful tool to aid identity theft victims and to preserve the integrity of consumer report data.

The FTC recognizes the benefits of an identity theft report, but also notes concerns that the report could be abused by those who want to falsely block the reporting of negative, but accurate, information. To address these concerns, the FTC has included two additional elements to the definition of an identity theft report. First, the report must allege identity theft "with as much specificity as the consumer can provide." Second, the consumer reporting agency or the furnisher receiving the report is permitted a limited opportunity to request additional information.

Although we believe the FTC has provided for some valuable concepts in the definition of an "identity theft report", we do not believe that they will address the concerns identified by the FTC. We believe the FTC should require the report to be filed with a law enforcement agency as required by the statute; this law enforcement should have the jurisdiction and ability to investigate the crime. Adding this requirement would deter the filing of false reports with far away law enforcement agencies with no interest or jurisdiction to investigate the crime. The FTC identifies its own identity theft reporting system as an example that "illustrates the possibility for abuse" if it were to be used as a foundation for an identity theft report. For the reasons the FTC has provided, we agree that the FTC would not be an appropriate law enforcement agency with which to file an allegation of identity theft for purposes of the filing an "identity theft report." In light of the many law enforcement options available to the consumer, which include, but are not

limited to, the local police department, the Federal Bureau of Investigation, or the U.S. Postal Inspection Service, we do not believe such a requirement poses a legitimate hindrance to identity theft victims.

Obtaining Additional Information

The proposed rule would allow a furnisher or a consumer reporting agency to obtain additional information from the victim in connection with the submission of an identity theft report. We agree with this provision, however, we are concerned that this opportunity is limited to a single request for limited purposes. A furnisher or agency should be permitted to make the requests necessary for legitimate purposes, such as to ensure the appropriate information is blocked or to investigate the crime itself. Furthermore, we do not believe that five business days is sufficient for a furnisher to determine whether additional information is needed. We recommend that 30 days would be a more appropriate period of time.

Duration of Active Duty Alerts

Military personnel who meet the definition of an "active duty military consumer" may request that an active duty alert be placed in their credit files. This alert is intended to notify users of the military personnel's consumer report that the consumer is on active duty in order that potentially fraudulent activities may be responded to. The statute requires that an active duty alert remain in a consumer's file for at least twelve months, although the FTC may extend this timeframe. We agree with the proposed twelve-month time period for active duty alerts.

Conclusion

Fifth Third applauds the FTC for its efforts in providing clarity to the FACTA Identity Theft Rule, yet urges that revisions be made to focus requirements on actual identity theft. We appreciate the opportunity to comment on this proposal. Should you wish to discuss any elements of this letter further, please call me at (513) 534-7323.

Sincerely,

Michael Matossian
Chief Compliance Officer
Fifth Third

cc: Malcolm Griggs, Chief Risk Officer
Paul Reynolds, Chief Counsel